Asset Search

Danish Shakya

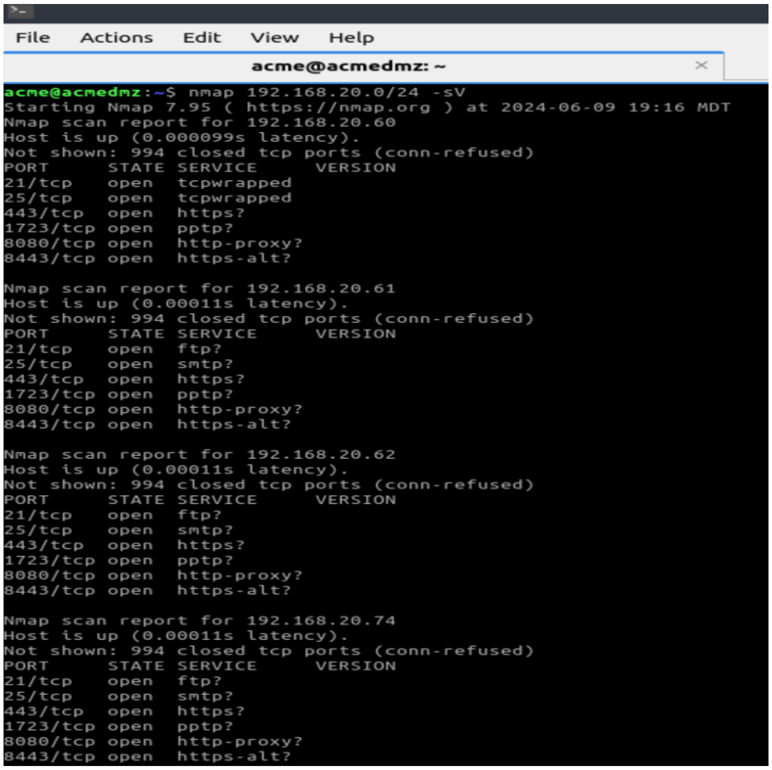
FLATIRON SCHOOL

Capstone

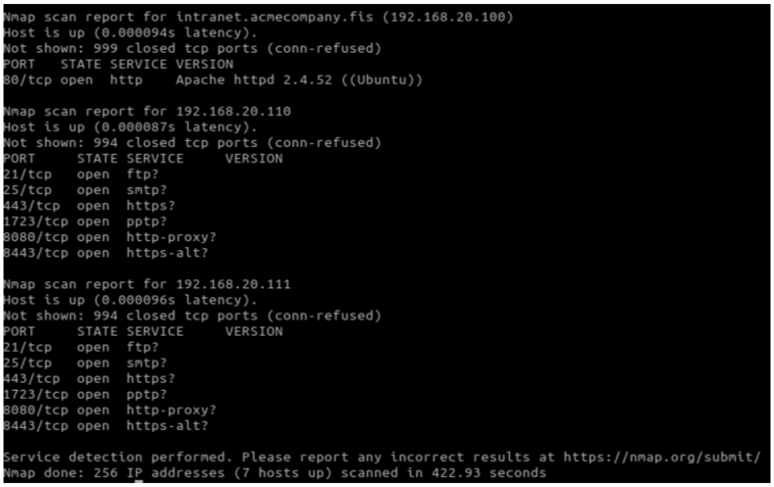
Network Asset Information:

1.ACME Security Server:

Nmap 192.168.20.0/24 -sV



```
acme@acmedmz:~$ nmap 192.168.20.0/24 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2024-06-09 19:16 MDT
Nmap scan report for 192.168.20.60
Host is up (0.000099s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  tcpwrapped
25/tcp   open  tcpwrapped
443/tcp  open  https?
1723/tcp open  pptp?
8080/tcp open  http-proxy?
8443/tcp open  https-alt?

Nmap scan report for 192.168.20.61
Host is up (0.00011s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp?
25/tcp   open  smtp?
443/tcp  open  https?
1723/tcp open  pptp?
8080/tcp open  http-proxy?
8443/tcp open  https-alt?

Nmap scan report for 192.168.20.62
Host is up (0.00011s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp?
25/tcp   open  smtp?
443/tcp  open  https?
1723/tcp open  pptp?
8080/tcp open  http-proxy?
8443/tcp open  https-alt?

Nmap scan report for 192.168.20.74
Host is up (0.00011s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp?
25/tcp   open  smtp?
443/tcp  open  https?
1723/tcp open  pptp?
8080/tcp open  http-proxy?
8443/tcp open  https-alt?
```

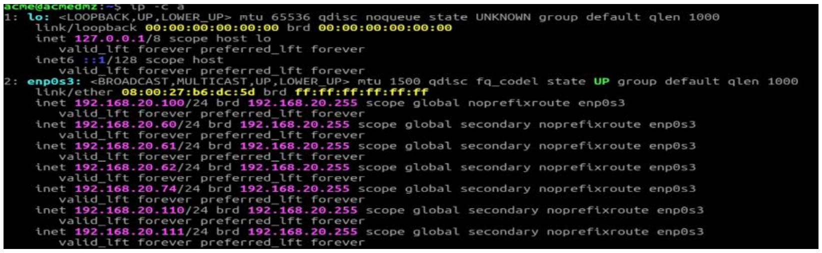


```
Nmap scan report for intranet.acmecompany.fis (192.168.20.100)
Host is up (0.000094s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))

Nmap scan report for 192.168.20.110
Host is up (0.000087s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp?
25/tcp   open  smtp?
443/tcp  open  https?
1723/tcp open  pptp?
8080/tcp open  http-proxy?
8443/tcp open  https-alt?

Nmap scan report for 192.168.20.111
Host is up (0.000096s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp?
25/tcp   open  smtp?
443/tcp  open  https?
1723/tcp open  pptp?
8080/tcp open  http-proxy?
8443/tcp open  https-alt?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (7 hosts up) scanned in 422.93 seconds
```

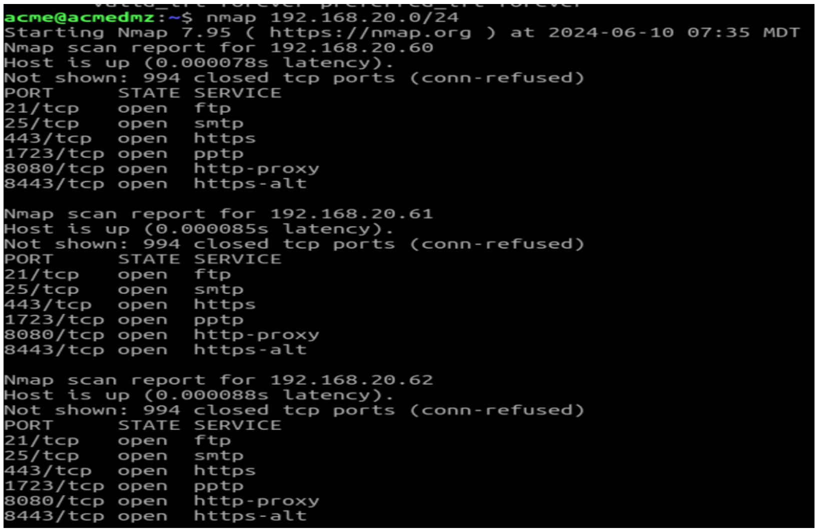
2.DMZ Linux Server:

Ip -c a

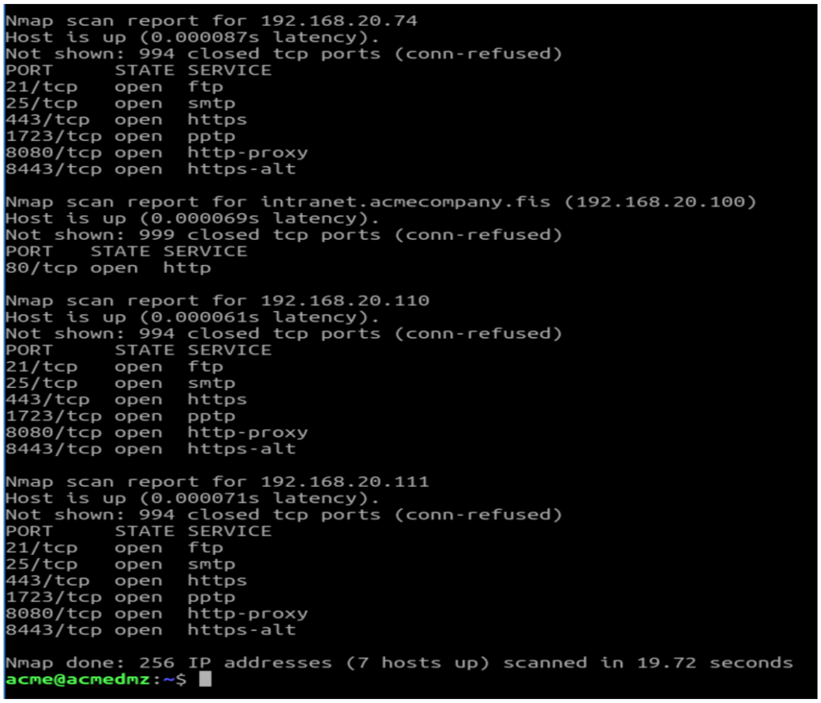
nmap 192.168.20.0/24



```
acme@acmedmz:~$ ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b6:dc:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.100/24 brd 192.168.20.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.20.60/24 brd 192.168.20.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.20.61/24 brd 192.168.20.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.20.62/24 brd 192.168.20.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.20.74/24 brd 192.168.20.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.20.110/24 brd 192.168.20.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.20.111/24 brd 192.168.20.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
```



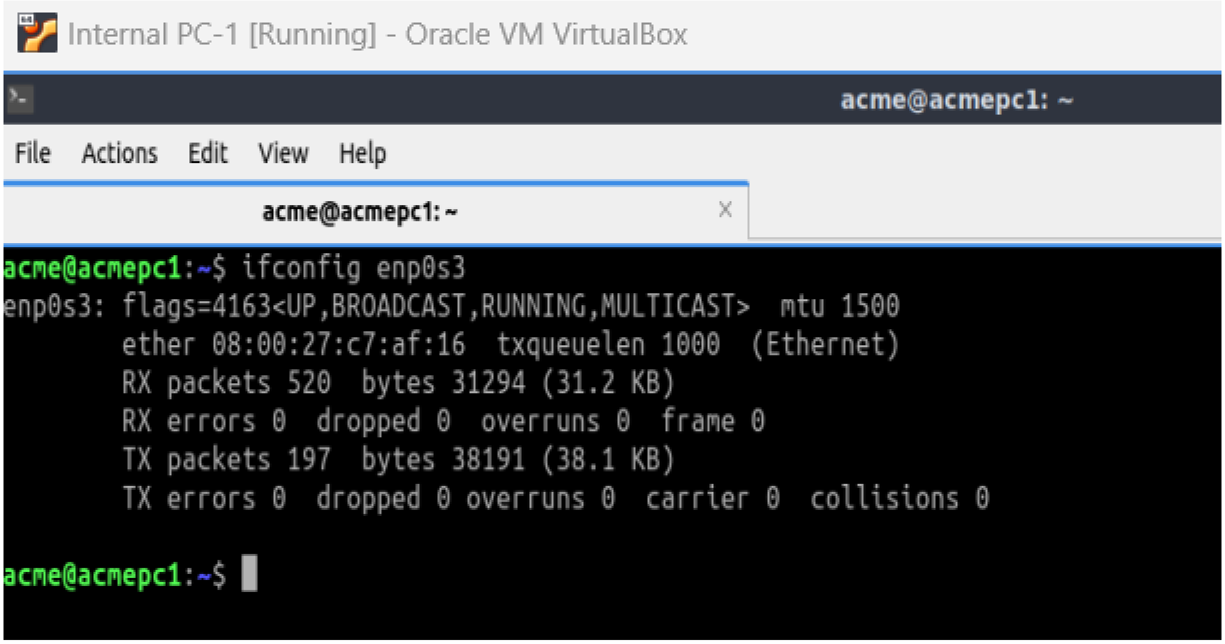
```
       valid_lft forever preferred_lft forever
acme@acmedmz:~$ nmap 192.168.20.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2024-06-10 07:35 MDT
Nmap scan report for 192.168.20.60
Host is up (0.000078s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
443/tcp  open  https
1723/tcp open  pptp
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap scan report for 192.168.20.61
Host is up (0.000085s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
443/tcp  open  https
1723/tcp open  pptp
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap scan report for 192.168.20.62
Host is up (0.000088s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
443/tcp  open  https
1723/tcp open  pptp
8080/tcp open  http-proxy
8443/tcp open  https-alt
```



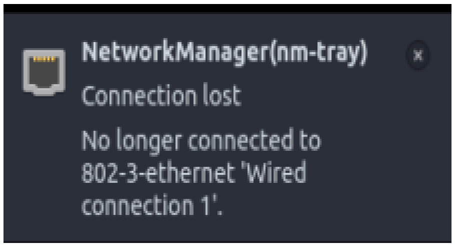
```
Nmap scan report for 192.168.20.74
Host is up (0.000087s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
443/tcp  open  https
1723/tcp open  pptp
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap scan report for intranet.acmecompany.fis (192.168.20.100)
Host is up (0.000069s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 192.168.20.110
Host is up (0.000061s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
443/tcp  open  https
1723/tcp open  pptp
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap scan report for 192.168.20.111
Host is up (0.000071s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
443/tcp  open  https
1723/tcp open  pptp
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 256 IP addresses (7 hosts up) scanned in 19.72 seconds
acme@acmedmz:~$ 
```

3.Internal PC-1:

The Internal PC-1 was not connected to the Network.


Internal PC-1 [Running] - Oracle VM VirtualBox
acme@acmepc1: ~
File Actions Edit View Help
acme@acmepc1: ~

```
acme@acmepc1:~$ ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:c7:af:16  txqueuelen 1000  (Ethernet)
        RX packets 520  bytes 31294 (31.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 197  bytes 38191 (38.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

acme@acmepc1:~$
```



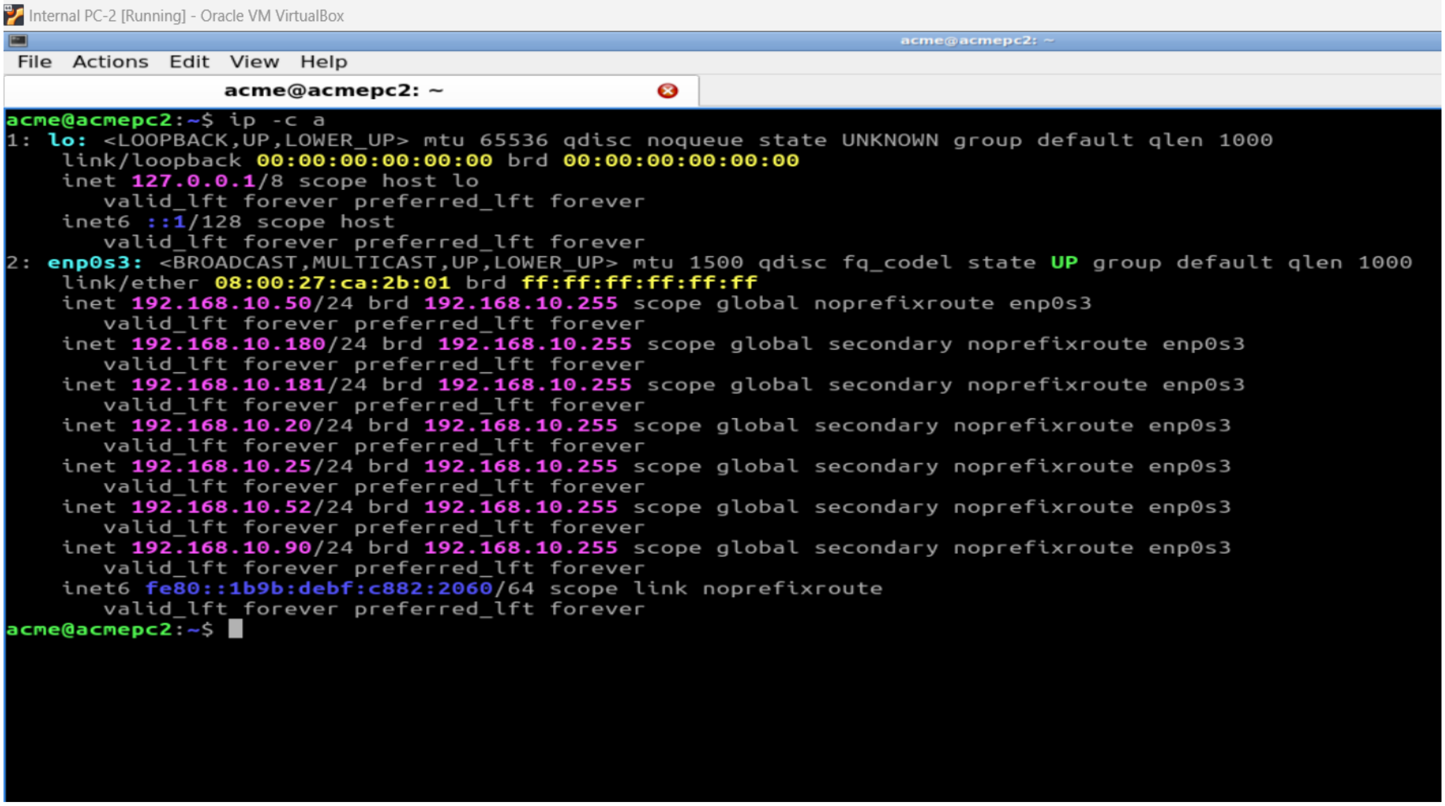
NetworkManager(nm-tray)

Connection lost

No longer connected to 802-3-ethernet 'Wired connection 1'.

4.Internal PC-2:

Ip -c a

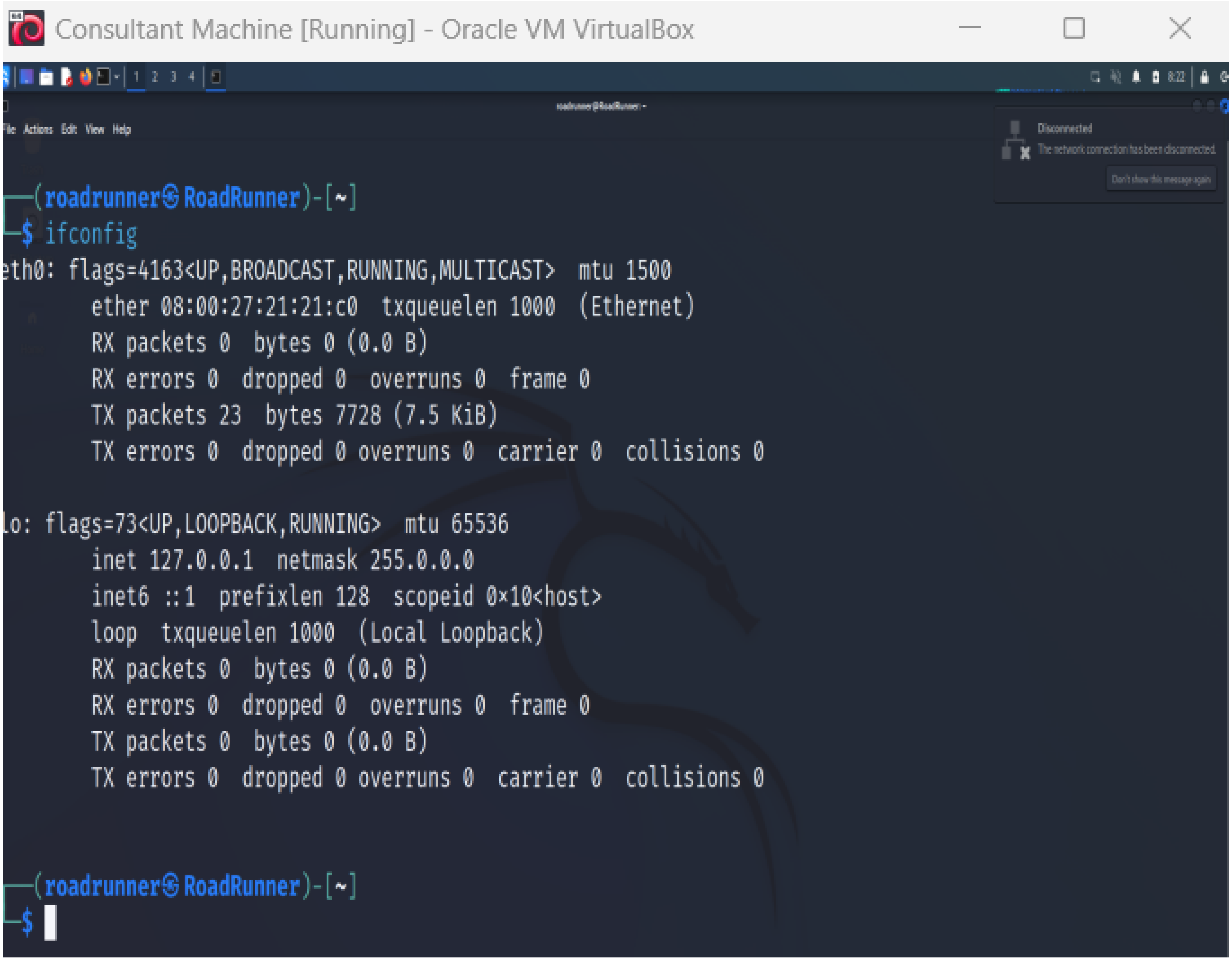

Internal PC-2 [Running] - Oracle VM VirtualBox
acme@acmepc2: ~
File Actions Edit View Help
acme@acmepc2: ~

```
acme@acmepc2:~$ ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ca:2b:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.50/24 brd 192.168.10.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.10.180/24 brd 192.168.10.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.10.181/24 brd 192.168.10.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.10.20/24 brd 192.168.10.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.10.25/24 brd 192.168.10.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.10.52/24 brd 192.168.10.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.10.90/24 brd 192.168.10.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::1b9b:debf:c882:2060/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
acme@acmepc2:~$
```

5.Consultant Machine:

Ifconfig

We had been notified that SOC Network is connected to 192.168.30.0/24) on intnet-3.


Consultant Machine [Running] - Oracle VM VirtualBox
roadrunner@RoadRunner: ~
File Actions Edit View Help
8:22
Don't show this message again

Disconnected

The network connection has been disconnected.

```
┌──(roadrunner㉿RoadRunner)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:21:21:c0  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 7728 (7.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(roadrunner㉿RoadRunner)-[~]
└─$ █
```